UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NORTH CAROLINA
WESTERN DIVISION

UNITED STATES OF AMERICA, v. DANIEL PATRICK BOYD, HYSEN SHERIFI, ANES SUBASIC, ZAKARIYA BOYD, DYLAN BOYD, JUDE KENAN MOHAMMAD, MOHAMMAD OMAR ALY HASSAN, and ZIYAD YAGHI, Defendants.	)	No. 5:09-CR-216-FL

(U) GOVERNMENT'S COMBINED *REDACTED* MEMORANDUM IN OPPOSITION TO DEFENDANTS SHERIFI, SUBASIC, ZAKARIYA BOYD, DYLAN BOYD, AND HASSAN'S MOTIONS TO SUPPRESS FISA-DERIVED EVIDENCE AND TO COMPEL DISCLOSURE OF FISA APPLICATIONS AND ORDERS, AND DEFENDANT YAGHI'S MOTION TO SUPPRESS FISA-DERIVED EVIDENCE

TABLE OF CONTENTS

I. INTRODUCTION

The Government is filing this classified memorandum in opposition to: (1) Defendant Hysen Sherifi's Motion to Suppress FISA Evidence and Motion to Compel Disclosure of FISA Material, which has been adopted by Defendant Mohammad Omar Aly Hassan; (2) Defendant Anes Subasic's Motion to Suppress FISA Derived Evidence and Motion for Disclosure of FISA Applications and Orders; (3) defendants Zakariya Boyd and Dylan Boyds' Motion to Suppress FISA Evidence and to Compel Production of Government's FISA Application; and (4) Defendant Ziyad Yaghi's Motion to Suppress Evidence (collectively, "defendants' motions"). In essence, defendants' motions seek: (1) disclosure of all applications, orders, and related materials obtained pursuant to the Foreign Intelligence Surveillance Act, as amended ("FISA"),[1] (collectively, the "FISA materials");[2] and (2) suppression of information obtained or derived pursuant to FISA.

The Government expects that the Court will conclude from its *in camera, ex parte* review of the relevant FISA materials that the FISA electronic surveillance and physical searches at issue in this case were lawfully authorized and conducted, and that the FISA dockets should not be disclosed. For the reasons set forth below, the Court should deny the defendants' motions.

A. BACKGROUND

On November 24, 2010, defendants were charged in a thirteen-count superseding indictment with, *inter alia,* conspiracy to provide material support to terrorists, in violation of

[1] The provisions of FISA that deal with electronic surveillance are located at 50 U.S.C. §§ 1801-1812; those that deal with physical searches are located at 50 U.S.C. §§ 1821-1829. The two sets of provisions are in many respects parallel and almost identical. Citations herein are generally to the two sets of provisions in parallel, with the first citation being to the relevant electronic surveillance provision, and the second citation being to the relevant physical search provision.

[2] The FISA materials that the defendants have moved the Court to disclose in this case include the Government's underlying applications for authorization for electronic surveillance and physical search under FISA and any resulting

Title 18, United States Code, Section 2339A, and conspiracy to murder, kidnap, maim and injure persons, in violation of Title 18, United States Code, Section 956(a). The indictment is based upon the defendants' activities in preparation for violent jihad such as weapons training and overseas travel, in addition to their recruitment of and financial support for others to engage in terrorist activities. At trial, the Government intends to introduce against the defendants information obtained or derived from electronic surveillance and physical searches conducted pursuant to FISA.

On July 27, 2009, the Government provided written notice to the Court and to the defendants pursuant to 50 U.S.C. §§ 1806(c) and 1825(d), that the United States "intends to offer into evidence or otherwise use or disclose in any proceedings in the above-captioned matter, information obtained and derived from electronic surveillance and physical search conducted pursuant to the Foreign Intelligence Surveillance Act of 1978, as amended, 50 U.S.C. §§ 1801-1811, 1821-1829." *See* docket entries 34-40 in this proceeding.

In opposition to defendants' motions, the Government [submitted a classified memorandum of law for the Court's *in camera* and *ex parte* review. This is an unclassified version of the classified memorandum].[3] In addition, the Government is filing herewith the following documents in support of its opposition: (1) an unclassified Declaration and Claim of Privilege of the Attorney General of the United States, explaining that disclosure of the FISA dockets would harm the national security of the United States (attached hereto as Exhibit 1).

---

orders authorizing collection under FISA.

[3] As a result of the redactions, the pagination and footnote numbering of the classified memorandum and the unclassified memorandum are different.

The Government's pleadings and the supporting FISA materials are submitted not only to oppose the defendants' motions, but also to support the United States' request, pursuant to FISA, that this Court: (1) conduct an *in camera* and *ex parte* review of the FISA materials; (2) find that the FISA collection at issue was lawfully authorized and conducted; and (3) order that none of the classified documents, nor any of the classified information contained therein, be disclosed to the defense, and instead, that they be maintained by the United States under seal.

B. OVERVIEW OF THE FISA COLLECTION AT ISSUE

II. THE FISA PROCESS

A. OVERVIEW OF FISA

Enacted in 1978, and subsequently amended, FISA authorizes the Chief Justice of the United States to designate eleven United States District Judges to sit as judges of the FISC. 50 U.S.C. § 1803(a)(1). The FISC judges are empowered to consider *ex parte* applications submitted by the Executive Branch for electronic surveillance and physical search when a significant purpose of the application is to obtain foreign intelligence information, as defined in FISA. Rulings of the FISC are subject to review by the Foreign Intelligence Surveillance Court of Review ("FISC of Review"), which is composed of three United States District or Circuit Judges designated by the Chief Justice. 50 U.S.C. § 1803(b). As discussed below, a District Court also has jurisdiction to determine the legality of electronic surveillance and physical searches authorized by the FISC when the fruits of that intelligence collection are used against an "aggrieved person."[4] *See* 50 U.S.C. §§ 1806(f), 1825(g).

[4] An "aggrieved person" is defined as the target of electronic surveillance or "any other person whose communications or activities were subject to electronic surveillance," 50 U.S.C. § 1801(k), as well as "a person whose premises, property, information, or material is the target of physical search" or "whose premises, property, information, or material was subject to physical search. 50 U.S.C. § 1821(2). The defendants are "aggrieved

As originally enacted, FISA required that a high-ranking member of the Executive Branch of government certify that "the purpose" of the FISA application was to obtain foreign intelligence information. In 2001, FISA was amended as part of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (PATRIOT Act).[5] One change to FISA accomplished by the PATRIOT Act is the abrogation of the requirement that the primary purpose of the requested FISA surveillance be the gathering of foreign intelligence information; instead, a high-ranking official is now to certify that the acquisition of foreign intelligence information is "a significant purpose" of the requested surveillance. 18 U.S.C. § 1804(a)6)(B). As discussed in detail in later sections of this memorandum, the "significant purpose" standard is constitutional.

B. THE FISA APPLICATION

FISA provides a statutory procedure whereby the Executive Branch may obtain a judicial order or warrant authorizing the use of electronic surveillance and/or physical search within the United States where a significant purpose is the collection of foreign intelligence information. *United States v. Johnson,* 952 F.2d 565, 571 (1st Cir. 1992); *United States v. Abu-Jihaad,* 630 F.3d 102, 117-118 (2d Cir. 2010); 50 U.S.C. §§ 1804(a)(6)(B), 1823(a)(6)(B). Under FISA, "[f]oreign intelligence information" includes information that "relates to, and if concerning a United States person[6] is necessary to, the ability of the United States to protect against . . . actual

---

persons" under FISA, and as noted above, they were provided with notice of their status as such and of the Government's intent to use FISA-obtained or -derived information against them at trial.

[5] Pub. L. No. 107-56, 115 Stat. 271 (2001).

[6] Under FISA, a "United States person" means a citizen of the United States, an alien lawfully admitted for permanent residence as defined in Section 101(a)(20) of the Immigration and Nationality Act, an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or association which is a foreign power, as defined in 50 U.S.C. §§ 8801(a)(1), (2), or (3). 50 U.S.C. § 1801(i), 50

or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power [and/or] sabotage or international terrorism by a foreign power or an agent of a foreign power." 50 U.S.C. §§ 1801(e), 1821(1). "Foreign intelligence information" also includes information with respect to a "foreign power or foreign territory that relates to, and if concerning a United States person is necessary to – (A) the national defense or the security of the United States; or (B) the conduct of the foreign affairs of the United States." 50 U.S.C. §§ 1801(e)(2), 1821(1). With the exception of emergency authorizations, FISA requires that a court order be obtained before any electronic surveillance or physical search may be conducted.[7]

An application to conduct electronic surveillance pursuant to FISA must contain, among other things: (1) the identity of the federal officer making the application; (2) the identity, if known, or a description of the specific target of the electronic surveillance; (3) a statement of the facts and circumstances supporting probable cause to believe that the target is a foreign power or an agent of a foreign power, and that each facility or place at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power; (4) a statement of the proposed minimization procedures to be followed; (5) a detailed description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance; (6) a certification, discussed below, of a high-ranking official; (7) the manner or means by which the electronic surveillance or physical search will be effected and a statement whether physical entry is required to effect the electronic surveillance; (8) the facts concerning and the action taken on all previous FISA applications involving any of the persons,

---

U.S.C. § 1821(1). All of the targets are United States persons.

[7] As noted above, FISA provides that in emergency situations the Attorney General may authorize electronic surveillances or physical searches without an order from the FISC. See 50 U.S.C. §§ 1805(e), 1824(e).

facilities, places, premises or property specified in the application; and (9) the proposed duration of the electronic surveillance or physical search. *See* 50 U.S.C. § 1804(a)(1)-(9).

An application to conduct a physical search pursuant to FISA must contain similar information as an application to conduct electronic surveillance. *See* 50 U.S.C. § 1823(a)(1)-(8). The primary difference is that an application to conduct a physical search must also contain a statement of the facts and circumstances supporting probable cause to believe that "the premises or property to be searched contains foreign intelligence information" and that "each premises or property to be searched is owned, used, possessed by, or is in transit to or from" the target. *See* 50 U.S.C. §§ 1823(a)(3)(B), (C).

1. The Certification

An application to the FISC for a FISA order or warrant must include a certification from a high-ranking Executive Branch official with national security responsibilities that:

> (A) the certifying official deems the information sought to be foreign intelligence information;
>
> (B) a significant purpose of the surveillance is to obtain foreign intelligence information;
>
> (C) such information cannot reasonably be obtained by normal investigative techniques;
>
> (D) designates the type of foreign intelligence information being sought according to the categories described in 50 U.S.C. § 1801(e); and
>
> (E) includes a statement of the basis for the certification that –
>
> > (i) the information sought is the type of foreign intelligence information designated; and
> >
> > (ii) such information cannot reasonably be obtained by normal investigative techniques.

50 U.S.C. § 1804(a). *See also* 50 U.S.C. § 1823(a).

2. Minimization Procedures

The Attorney General has adopted, and the FISC has approved, minimization procedures that regulate the acquisition, retention, and dissemination of information obtained through FISA collection about United States persons, including persons who are not the targets of the FISA collection. FISA requires that such minimization procedures must be:

> reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.

50 U.S.C. § 1801(h)(1); *see also* 50 U.S.C. § 1821(4)(A) (same regarding physical search).

In addition, minimization procedures also include "procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes." 50 U.S.C. § 1801(h)(3); *see also* 50 U.S.C. § 1821(4)(c) (same regarding physical search).

In order to fulfill the statutory requirements discussed above, the Attorney General has adopted standard minimization procedures ("SMP"s) for FISC-authorized electronic surveillance and physical search that are on file with the FISC and are incorporated by reference into every relevant FISA application that is submitted to the FISC.[8] As a result, the FISC judges who issued the orders authorizing the FISA collection at issue here found that the applicable standard minimization procedures, as well as any supplemental minimization procedures that may have

[8] As discussed in detail in a later section, there are two sets of SMPs that are applicable to the FISA applications at issue, and both sets are submitted for this Court's *in camera, ex parte* review in the Sealed Exhibit.

been proposed, met FISA's statutory requirements. The FISC orders in the dockets at issue here directed the Government to follow the approved minimization procedures in conducting the FISA collection.

3. Attorney General's Approval

FISA further requires that the Attorney General[9] approve applications for electronic surveillance and/or physical search before they are presented to the FISC. *Id.*

C. THE FISC'S ORDERS

Once approved by the Attorney General, the application is submitted to the FISC and assigned to one of its judges. The FISC may approve the requested electronic surveillance or physical search only upon finding, among other things, that: (1) the application has been made by a "Federal officer" and has been approved by the Attorney General; (2) there is probable cause to believe that (a) the target of the electronic surveillance and/or physical search is a foreign power or an agent of a foreign power, and that (b) the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power [or that the premises or property to be searched is owned, used, possessed by, or is in transit to or from a foreign power or an agent of a foreign power]; (3) the proposed minimization procedures meet the statutory requirements set forth in 50 U.S.C. § 1801(h) (electronic surveillance) and/or 50 U.S.C. § 1821(4) (physical search); (4) the application contains all of the statements and certifications required by Section 1804 or Section 1823; and (5) if the

---

[9] As noted above, "Attorney General" means the Attorney General of the United States (or Acting Attorney General), the Deputy Attorney General, or, upon the designation of the Attorney General, the Assistant Attorney General designated as the Assistant Attorney General for National Security. See 50 U.S.C. § 1801(g)

target is a United States person – as defined above -- that the certifications are not clearly erroneous. 50 U.S.C. §§ 1805(a)(1)-(4), 1824(a)(1)-(4).

FISA defines "foreign power" to include "a group engaged in international terrorism or activities in preparation therefore " 50 U.S.C. §§ 1801(a)(4), 1821(1). As it relates to United States persons, "agent of a foreign power" includes any person who:

> (C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power;
>
> * * * * * * *
>
> or
>
> (E) knowingly aids or abets any person in the conduct of activities described in [the subparagraphs above] . . . or knowingly conspires with any person to engage in activities described in [the subparagraphs above.]

50 U.S.C. §§ 1801(b)(2) (electronic surveillance), 1821(1) (physical search).

FISA specifies that no United States person may be considered a foreign power or an agent of a foreign power solely on the basis of activities protected by the First Amendment to the Constitution of the United States. 50 U.S.C. §§ 1805(a)(2)(A), 1824(a)(2)(A). Although protected First Amendment activities cannot form the sole basis for FISC-authorized electronic surveillance or physical search, they may be considered by the FISC if there is other activity indicative that the target is an agent of a foreign power. *United States v. Rosen*, 447 F.Supp.2d 538, 549-50 (E.D. Va. 2006); *United States v. Rahman*, 861 F.Supp. 247, 252 (S.D.N.Y. 1994), *aff'd* 189 F.3d 88 (2nd Cir. 1999). Additionally, FISA provides that "[i]n determining whether or not probable cause exists ... a judge may consider past activities of the target, as well as facts and

circumstances relating to current or future activities of the target." 50 U.S.C. §§ 1805(b), 1824(b).

If the FISC is satisfied that the FISA application has met the statutory provisions and has made all of the necessary findings, the FISC issues an *ex parte* order authorizing the electronic surveillance and/or physical search requested in the application. 50 U.S.C. §§ 1805(a), 1824(a). The order must specify: (1) the identity (or a description of) the specific target of the collection; (2) the nature and location of each facility or place at which the electronic surveillance will be directed or of each of the premises or properties to be searched; (3) the type of information sought to be acquired and the type of communications or activities to be subjected to the electronic surveillance, or the type of information, material, or property to be seized, altered, or reproduced through the physical search; (4) the means by which electronic surveillance will be effected and whether physical entry will be necessary to effect the surveillance, or a statement of the manner in which the physical search will be conducted; (5) the period of time during which electronic surveillance is approved and/or the authorized scope of each physical search; and (6) the applicable minimization procedures. 50 U.S.C. §§ 1805(c)(1), 1824(c)(1). The FISC also retains the authority to review, before the end of the authorized period of electronic surveillance or physical search, the United States' compliance with the requisite minimization procedures. 50 U.S.C. §§ 1805(d)(3), 1824(d)(3).

Under FISA, electronic surveillance and/or physical searches targeting a United States person may be approved for up to ninety days. 50 U.S.C. §§ 1805(d)(1), 1824(d)(1). Extensions may be granted, but only if the United States submits another application in compliance with FISA. 50 U.S.C. §§ 1805(e)(2), 1824(d)(2).

III. DISTRICT COURT REVIEW OF FISC ORDERS

FISA authorizes the use in a criminal prosecution of information obtained or derived from any FISC-authorized electronic surveillance and/or physical search, provided that advance authorization is obtained from the Attorney General, *see* 50 U.S.C. §§ 1806(b), 1825(c), and that proper notice is given to the court and to each aggrieved person against whom the information is to be used, *see* 50 U.S.C. §§ 1806(c), (d), and 1825(d), (e). Upon receiving notice, an aggrieved person may then move to suppress the use of FISA information on two grounds: (1) that the information was unlawfully acquired under FISA; or (2) that the electronic surveillance or physical search was not conducted in conformity with the FISC's order(s). 50 U.S.C. §§ 1806(e), 1825(f). Accordingly, as discussed in detail in later sections, suppression motions are evaluated using FISA's probable cause standard, not the probable cause standard for criminal warrants. *See, e.g., United States v. Pelton,* 835 F.2d 1067, 1075 (4th Cir. 1987).

When the Government has served notice on an aggrieved person of its intent to use FISA-obtained or –derived information against that person, he or she has standing to challenge the lawfulness of the FISA surveillance and/or search. In that event, the district court in which the matter is pending has jurisdiction to determine the legality of the electronic surveillance and/or physical search. *See* 50 U.S.C. §§ 1806(f), 1825(g).

A. THE REVIEW IS TO BE CONDUCTED *IN CAMERA* AND *EX PARTE*

In assessing the legality of challenged FISA surveillance or searches, the district court, "shall, notwithstanding any other law, if the Attorney General files [as he has filed in this proceeding] an affidavit or declaration under oath that disclosure or an adversary hearing would harm the national security of the United States, review *in camera* and *ex parte* the application,

order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted." 50 U.S.C. §§ 1806(f), 1825(g). On the filing of the Attorney General's affidavit or declaration, the court "may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order or other materials relating to the surveillance [or physical search] *only where such disclosure is necessary* to make an accurate determination of the legality of the surveillance [or search]."[10] 50 U.S.C. §§ 1806(f), 1825(g) (emphasis added). Thus, the propriety of the disclosure of any FISA applications or orders to the defendants cannot even be considered, unless and until the district court has first concluded that it is unable to make an accurate determination of the legality of the collection after reviewing the Government's submissions (and any supplemental pleadings that the district court may request) *in camera* and *ex parte*. *See Abu-Jihaad,* 630 F.3d at 129; *United States v. Belfield,* 692 F.2d 141, 147 (D.C. Cir. 1982); *United States v. Islamic American Relief Agency ("IARA"),* Case No. 07-00087-CR-W-NKL, 2009 WL 5169536, 2009 U.S. Dist. LEXIS 118505, at *10-11 (W.D.Mo. December 21, 2009); *United States v. Nicholson*, Case No. 09-CR-40-BR, 2010 WL 1641167, 2010 U.S. Dist. LEXIS 45126, at *9-10 (D. Or. April 21, 2010) ("After an *in-camera* review, the court 'has the discretion to disclose portions of the documents, under appropriate protective orders, *only if [the court] decides that such disclosure is necessary to make an accurate determination of the legality of the surveillance.' United States v. Duggan,* 743 F.2d 59, 78 (2d Cir. 1984) (emphasis

[10] In *Warsame*, 547 F.Supp.2d at 957, the court addressed the meaning of "necessary": "[t]he legislative history explains that such disclosure is 'necessary' only where the court's initial review indicates that the question of legality may be complicated" by factual misrepresentations, insufficient identification of the target, or failure to comply with the minimization standards in the order.

added)."); *United States v. Kashmiri*, Case No. 09-CR-830-4, 2010 WL 4705159, 2010 U.S. Dist. LEXIS 119470, at *6 (N.D. Ill., November 10, 2010).

If the district court is able to make an accurate determination of the legality of the surveillance based on its *in camera, ex parte* review of the materials submitted by the United States, then the court *may not* order disclosure of any of the FISA materials to the defense, unless otherwise required by due process. *United States v. Duggan*, 743 F.2d 59, 78 (2d Cir. 1984) (affirming district court's refusal to disclose FISA materials where the court was able to determine the legality of the surveillance without assistance from to the defense); *Kashmiri*, 2010 U.S. Dist. LEXIS 119470, at *6 ("If disclosure of the FISA materials is not necessary for the district court to make an accurate determination of the legality of the collection, disclosure *may not be ordered*" [emphasis in original]). Likewise, if this Court is able to determine the legality of the FISA collection, then there will be no hearing. "The demand for an adversary hearing must fall with the demand for disclosure of the *in camera* Exhibit. They are inextricably linked. [When] disclosure is not necessary, no purpose would be served by an evidentiary hearing." *Belfield*, 692 F.2d at 147.

Federal courts have repeatedly and consistently held that FISA "anticipates that an *in camera, ex parte* determination is to be the rule," with disclosure and an adversarial hearing being the "exception, occurring *only* when necessary." *Belfield*, 692 F.2d at 147 (emphasis in original); *Abu Jihaad,* 630 F.3d at 129 ("[m]indful of these provisions, we have concluded that disclosure of FISA materials 'is the exception and *ex parte, in camera* determination is the rule.' *United States v. Stewart,* 590 F.3d [93,] 129 [2nd Cir. 2009]"); *Duggan*, 743 F.2d at 78; *Rosen*, 447 F.Supp.2d at 546; *Nicholson,* U.S.Dist.LEXIS at 2 ("disclosure of FISA materials to defense

counsel is not the rule"); *United States v. Spanjol*, 720 F.Supp. 55, 59 (E.D. Pa 1989), *aff'd* 958 F.2d 365 (3rd Cir. 1992) (*in camera, ex parte* procedure has been "uniformly followed by all Courts which have reviewed the legality of electronic surveillances authorized by the [FISC]"). Indeed, no court has ever found it necessary to disclose FISA materials to a criminal defendant to assist the court's determination of the lawfulness of either electronic surveillance or physical searches under FISA. *See United States v. Mubayyid*, 521 F.Supp.2d 125, 130 (D.Mass. 2007) (collecting cases); *Rosen*, 447 F.Supp.2d at 546 (same); *United States v. Gowadia*, No. 05-00486, 2009 WL 1649714, 2009 U.S. Dist. LEXIS 47833, at *6 (D. Hawaii June 8, 2009) ("to date, no court has held that disclosure of the FISA application papers was necessary in order to determine the lawfulness of a search authorized under FISA"); *Kashmiri*, 2010 U.S. Dist. LEXIS 119470, at *7 ("A court has never permitted defense counsel to review FISA materials"); *In re Grand Jury Proceedings of the Special April 2002 Grand Jury* ("*In re Grand Jury Proceedings*"), 347 F.3d 197, 203 (7th Cir. 2003) (noting that no court has ever ordered disclosure of FISA materials).

Every court that has addressed a motion to disclose FISA dockets or to suppress FISA materials has been able to reach a conclusion as to the legality of the FISA collection at issue based on an *in camera* and *ex parte* review. *See e.g., Spanjol,* 720 F.Supp. 58-59 ("The Court's *ex parte, in camera* review of the Sealed Exhibit submitted by the Attorney General is proper. It is well established that the legality of foreign intelligence surveillance should be determined on an *in camera, ex parte* basis"); *United States v. Nicholson*, 955 F.Supp. 588, 592 n. 11 (E.D.Va 1997) ("this court knows of no instance in which a court has required an adversary hearing or disclosure in determining the legality of a FISA surveillance") (collecting cases); *Thomson*, 752 F.Supp. 75, 79 (W.D.N.Y. 1990) (same); *United States v. Abu-Jihaad,* 531 F. Supp. 2d 299, 310

(D. Conn. 2008) (courts have uniformly held that such review procedures do not deprive a defendant of due process); *Mubayyid,* 521 F. Supp. 2d at 130; *Rosen,* 447 F. Supp. 2d at 546; *United States v. Isa,* 923 F.2d 1300, 1307 (8th Cir. 1991) (FISA's review procedures do not violate a defendant's Sixth Amendment confrontation rights);

There is nothing extraordinary about the FISA collections authorized here that would justify this case becoming the first "exception" to the rule of more than two decades of FISA litigation - that is, the first-ever to order the production and disclosure of highly sensitive and classified FISA dockets. Here, the FISA dockets are well-organized and easily reviewable by the Court *in camera* and *ex parte.* In addition, they are fully and facially sufficient to allow the Court to make an accurate determination of the legality of the FISA collection; indeed, they "are straightforward and readily understood." *In re Kevork,* 634 F. Supp. 1002, 1008 (C.D. Cal. 1985), *aff'd,* 788 F.2d 566 (9th Cir. 1986). Moreover, as in other cases, "[t]he determination of legality in this case is not complex." *Belfield,* 692 F.2d at 147; *see also Warsame,* 547 F. Supp. 2d at 987 ("issues presented by the FISA applications are straightforward and uncontroversial"); *Abu-Jihaad,* 531 F. Supp. 2d at 310 (district court review of FISA dockets was "relatively straightforward and not complex"); *Thomson,* 752 F. Supp. at 79 (no disclosure of FISA dockets warranted under Section 1806(f) where issues were "not so complex that the participation of the defendant [was] required to accurately determine the legality of the surveillance at issue"). The Government respectfully submits that this Court, much like the aforementioned courts, is able to review the FISA dockets *in camera* and *ex parte.*

In addition to the specific harm that would result from the disclosure of the FISA dockets in this case, which is detailed in the classified Declaration of a high-ranking FBI official in

support of the Attorney General's Declaration and Claim of Privilege, the underlying rationale for non-disclosure is clear: "In the sensitive area of foreign intelligence gathering, the need for extreme caution and sometimes even secrecy may not be overemphasized." *United States v. Ott,* 637 F. Supp. 62, 65, *aff'd* 827 F.2d 473,477 (9th Cir. 1987) ("Congress has a legitimate interest in authorizing the Attorney General to invoke procedures designed to ensure that sensitive security information is not unnecessarily disseminated to anyone not involved in the surveillance operation in question."); *accord IARA*, 2009 U.S. Dist. LEXIS 118505, at *8-9.

Confidentiality is critical to national security. "If potentially valuable intelligence sources" believe that the United States will be "unable to maintain the confidentiality of its relationship to them," then those sources "could well refuse to supply information." *CIA v. Sims,* 471 U.S. 159, 174 (1985); *see also Phillippi v. CIA,* 655 F.2d 1325, 1332-33 (D.C. Cir. 1981) (noting that a disclosure order relating to other highly sensitive and classified sources could chill the willingness of such sources to share information with the United States in the future). When a question is raised as to whether the disclosure of classified sources, methods, techniques, or information would harm the national security, Federal courts have expressed a great reluctance to replace the considered judgment of Executive Branch officials charged with the responsibility of weighing a variety of subtle and complex factors in determining whether the disclosure of information may lead to an unacceptable risk of compromising the intelligence gathering process, and determining whether foreign agents, spies, and terrorists are capable of piecing together a mosaic of information that, when revealed, could reasonably be expected to harm the national security of the United States. *See Sims,* 471 U.S. at 180; *United States v. Yunis,* 867 F.2d 617, 623 (D.C. Cir. 1989) ("Things that did not make sense to the District Judge would make all too

much sense to a foreign counter-intelligence specialist who could learn much about this nation's intelligence-gathering capabilities from what these documents revealed about sources and methods."); *Halperin v. CIA,* 629 F.2d 144, 150 (D.C. Cir. 1980) ("each individual piece of intelligence information, much like a piece of jigsaw puzzle, may aid in piecing together other bits of information even when the individual piece is not of obvious importance in itself"). An adversary hearing is not only entirely unnecessary to aid the Court in the straightforward task before it, but such a hearing would *create* potential dangers that courts have consistently sought to avoid.

As the *Belfield* court explained:

> Congress recognized the need for the Executive to engage in and employ the fruits of clandestine surveillance without being constantly hamstrung by disclosure requirements. The statute is meant to "reconcile national intelligence and counterintelligence needs with constitutional principles in a way that is consistent with both national security and individual rights." In FISA the privacy rights of individuals are ensured not through mandatory disclosure, but through its provisions for in- depth oversight of FISA surveillance by all three branches of government and by a statutory scheme that to a large degree centers on an expanded conception of minimization that differs from that which governs law enforcement surveillance.

692 F.2d at 148 (footnotes and citations omitted); *see also ACLU Foundation of So. Cal. v. Barr ("ACLU Foundation"),* 952 F.2d 457, 465 (D.C. Cir. 1991) (citing *Belfield* for the proposition that Section 1806(f) "is an acceptable means of adjudicating the constitutional rights of persons who have been subjected to FISA surveillance").

B. *IN CAMERA, EX PARTE* REVIEW IS CONSTITUTIONAL

The constitutionality of FISA's *in camera, ex parte* review provisions has been affirmed by every Federal court that has considered the matter. *See, e.g., Abu-Jihaad,* 530 F.3d at 117;

Spanjol, 55 F.Supp. at 58; *United States v. Damrah,* 412 F.3d 618, 624 (6th Cir. 2005) ("FISA's requirement that the district court conduct an ex parte, in camera review of FISA materials does not deprive a defendant of due process."); *United States v. Ott,* 827 F.2d 473, 476-77 (9th Cir. 1987) (FISA's review procedures do not deprive a defendant of due process); *Gowadia,* 2009 U.S. Dist. LEXIS 47833, at *6; *United States v. Jayyousi,* No. 04-60001, 2007 WL 851278, at *7 (S.D. Fla. Mar. 15, 2007);[11] *United States v. Benkahla,* 437 F. Supp. 2d 541, 554 (E.D. Va. 2006); *ACLU Foundation,* 952 F.2d at 465; *United States v. Megahey,* 553 F. Supp. 1180, 1194 (E.D.N.Y. 1982) ("*ex parte, in camera* procedures provided in 50 U.S.C. § 1806(f) are constitutionally sufficient to determine the lawfulness of the electronic surveillance at issue while safeguarding defendants' fourth amendment rights"); *United States v. Falvey,* 540 F. Supp. 1306, 1315-16 (E.D.N.Y. 1982) (a "massive body of pre-FISA case law of the Supreme Court, [the Second] Circuit and others" supports the conclusion that the legality of electronic surveillance should be determined on an *in camera, ex parte* basis); *Belfield,* 692 F.2d at 148-49; *Nicholson,* U.S. Dist. LEXIS 45126 at *8-9.

There remains an unbroken history of Federal court holdings that FISA's *in camera, ex parte* review provisions are entirely compatible with the requirements and protections of the Constitution. As stated by the United States District Court for the Northern District of Georgia, "[t]he defendants do not cite to any authority for [the proposition that FISA is unconstitutional] because there is none. Every court that has considered FISA's constitutionality has upheld the statute from challenges under the Fourth, Fifth, and Sixth Amendments." *United States v. Ahmed,*

[11] All *Jayyousi* citations herein are to Westlaw because they are from a Magistrate Judge's Report and Recommendation that was adopted and incorporated. Westlaw, but not Lexis, includes the Report and Recommendation with the court's opinion; however, the Lexis report of the case may be found at 2007 U.S. Dist. LEXIS 18310.

Case No. 1:06-CR-147-WSD-CGB, 2009 U.S. Dist. Lexis 120007, at *30 (N.D. Ga. March 19, 2009) (order denying defendants' motion to disclose and suppress FISA materials).

In summary, FISA mandates a process by which the district court must conduct an initial *in camera* and *ex parte* review of FISA applications, orders, and related materials in order to determine whether the FISA collection was lawfully authorized and lawfully conducted. Such *in camera, ex parte* review is the rule in such cases and that procedure is Constitutional. In this case, the Attorney General has filed the required declaration invoking that procedure, and has declared that disclosure or an adversary hearing would harm national security. Accordingly, an *in camera, ex parte* review by this Court is the appropriate venue in which to determine whether the FISA collection was lawfully authorized and conducted pursuant to FISA.

C. THE DISTRICT COURT'S SUBSTANTIVE REVIEW

The District Court conducts a *de novo* review of each FISA application. *United States v. Hammoud*, 381 F.3d 316, 332 (4th Cir. 2004), *rev'd on other grounds*, 543 U.S. 1097 (2005), *op. reinstated in pertinent part*, 405 F.3d 1034 (4th Cir. 2005). The district court's review should determine: (1) whether the certifications submitted by the Executive Branch in support of the FISA application were properly made; (2) whether probable cause existed to authorize the electronic surveillance and/or physical search at issue; and (3) whether the collection was properly minimized. *See Abu-Jihaad*, 630 F.3d at 130-31.

1. Certifications are Subject to Only Minimal Scrutiny

Certifications submitted in support of a FISA application should be "subjected to only minimal scrutiny by the courts," *United States v. Badia*, 827 F.2d 1458, 1463 (11th Cir.

1987), and are "presumed valid." *Duggan*, 743 F.2d at 77 & n.6 (citing *Franks v. Delaware*, 438 U.S. 154, 171 (1978)); *Nicholson*, U.S.Dist.LEXIS 45126 at *13; *accord United States v. Campa*, 529 F.3d 980, 993 (11th Cir. 2008); *Warsame*, 547 F.Supp. 2d at 990 ("a presumption of validity [is] accorded to the certifications"). When a FISA application is presented to the FISC, "[t]he FISA Judge, in reviewing the application, is not to second-guess the executive branch official's certification that the objective of the surveillance is foreign intelligence information." *Duggan*, 743 F.2d at 77. Likewise, Congress intended that the reviewing district court should "have no greater authority to second-guess the executive branch's certifications than has the FISA judge." *Id.; see also, In re Grand Jury Proceedings,* 347 F.3d at 204-05; *Badia,* 827 F.2d at 1463; *Rahman,* 861 F.Supp. at 250; *IARA*, 2009 U.S. Dist. LEXIS 118505, at *13; *Kashmiri*, 2010 U.S. Dist. LEXIS 119470, at *4.

The district court's review should determine whether the certifications were made in accordance with FISA's requirements. *See Ahmed,* 2009 U.S. Dist. LEXIS 120007, at *20 ("the [c]ourt is not to second-guess whether the certifications were correct, but merely to ensure they were properly made"); *see also Campa,* 529 F.3d at 993 ("in the absence of a *prima facie* showing of a fraudulent statement by the certifying officer, procedural regularity is the only determination to be made if a non-United States person is the target"). If the target is a United States person, then the district court should also ensure that each certification is not "clearly erroneous." *Id.*. at 994; *Duggan*, 743 F.2d at 77; *Kashmiri*, 2010 U.S. Dist. LEXIS 119470, at *6. A certification is clearly erroneous only when "the reviewing court on the [basis of the] entire evidence is left with the definite and firm conviction that a mistake has been committed." *United States v. U.S.*

Gypsum Co., 333 U.S. 364, 395 (1948); *see United States v.Garcia,* 413 F.3d 201, 222 (2d Cir. 2005); *IARA*, 2009 U.S. Dist. LEXIS 118505, at *12.

2. FISA's "Significant Purpose" Standard is Constitutional

As noted above, FISA originally required that a high-ranking member of the Executive Branch certify that "the purpose" of the FISA application was to obtain foreign intelligence information. In 2001, FISA was amended by the PATRIOT Act, which *inter alia* deleted "the purpose" language, and instead substituted the requirement that the official certify that "a significant purpose" of the requested surveillance is to obtain foreign intelligence information. 18 U.S.C. § 1804(a)6)(B).

The primary purpose test was originally derived from consideration of warrantless searches that were conducted pursuant to the Executive's Article II foreign-affairs powers prior to the enactment of FISA. See e.g., *Abu Jihaad*,630 F.3d at 121. In that context, warrantless surveillance would be conducted as an exception to the Fourth Amendment, and would therefore be limited to the scope of the Constitution's grant of authority to the Executive to conduct foreign affairs. Prior to the PATRIOT Act's amendment of FISA, several courts imported the primary-purpose test from warrantless surveillance into the statutory interpretation of FISA's certification requirement. *See, Duggan*, 743 F.2d at 77; *Pelton*, 835 F.2d at 1075-76; *Badia*, 827 F.2d at 1464; *Johnson*, 952 F.2d at 572.[12] However, none of those cases held that the primary-purpose test was constitutionally mandated.[13] The Second Circuit explicitly stated, "we note that when, in *Duggan*,

[12] In *Johnson*, the First Circuit actually construed the purpose requirement in the negative, holding that "the investigation of criminal activity cannot be the primary purpose" of FISA surveillance. *Id.*

[13] The Ninth Circuit took a contrary view and hesitated to define FISA's purpose requirement "to draw too fine a distinction between criminal and intelligence investigations," because by definition international terrorism requires the investigation of some activities that also constitute crimes. *United States v. Sarkissian*, 841 F.2d 959, 965 (9th Cir.

we construed FISA's original reference to electronic surveillance for 'the purpose' of obtaining foreign intelligence information, as a 'requirement that foreign intelligence information be the *primary* objective . . . we were identifying Congress's intent in enacting FISA, not a constitutional mandate. . . . In short, nothing in *Duggan* erected a constitutional bar to Congress reconsidering and reframing the purpose requirement of FISA". *Abu Jihaad,*630 F.3d at 123.

With the exception of the now-vacated and legally null *Mayfield v. United States*, 504 F.Supp.2d 1023 (D. Or. 2007),[14] each court to have considered the PATRIOT Act amendment setting forth the significant-purpose test has held this test to be Constitutional. *See, In re Sealed Case*, 310 F.3d 717, 746 (FISC of Rev. 2002)[15]; *Abu Jihaad,* 630 F.3d at 128 ("We conclude simply that FISA's 'significant purpose' requirement . . . is sufficient to ensure that the executive may only use FISA to obtain a warrant when it is in good faith pursuing foreign intelligence gathering [and the] fact that the government may also be pursuing other purposes, including gathering evidence for criminal prosecution, compels no different conclusion"); *United States v. Ning Wen*, 477 F.3d 896, 897 (7th Cir. 2007); *Warsame*, 547 F.Supp.2d at 992-97; *Mubayyid,*521 F.Supp.2d at 139; *United States v. Marzook*, 435 F.Supp.2d 778, 786 (N.D. Ill. 2006); *Benkahla* 437 F.Supp.2d at 554; *Jayyousi*, 2007 WL 851278, at *1.

3. Probable Cause

1988).

[14] FISA's "significant purpose" standard was held unconstitutional in *Mayfiield*, a the civil case, which no other court followed and the Ninth Circuit eventually vacated on the ground that the plaintiff lacked standing. *See Mayfield v. United States*, 588 F.3d 1252 (9th Cir. 2009). And, as is the case for the lower court's decision in *Mayfield*, when a judgment is vacated by a higher court "it deprives the [lower] court's opinion of precedential effect." *Los Angeles County v. Davis*, 440 U.S. 625, 634 n. 6 (1979). Moreover, the district court's rational in *Mayfield* was specifically rejected in *Kashmiri*, 2010 U.S. Dist. LEXIS 119470, at *8.

[15] "FISC of Rev." refers to the Foreign Intelligence Surveillance Court of Review, which is the specialized federal appellate court that Congress established to hear appeals from the FISC.

FISA requires a finding of probable cause that the target is a foreign power or an agent of a foreign power and that each facility or property at which the electronic surveillance and/or physical search is directed is being used, owned, and/or possessed, or is about to be used, owned, and/or possessed, by a foreign power or an agent of a foreign power.. It is this standard, not the standard applicable to a criminal search warrant, that this Court must apply. *See Abu-Jihaad*, 630 F.3d at 130-31; *Cavanagh,* 807 F.2d. at 790 (citing *United States v. United States District Court (Keith),* 407 U.S. 297, 322 (1972)). This "different, and arguably lower, probable cause standard . . . reflects the purpose for which FISA search orders are issued." *Ahmed,* 2009 U.S. Dist. LEXIS 120007, at *22.

a. The Fourth Amendment

Courts have universally agreed that FISA's probable cause standard comports with the Fourth Amendment. *See, e.g. Isa*, 923 F.2d at 1304. FISA's probable cause requirement was crafted by Congress with an eye towards the Fourth Amendment and in recognition of the unique nature and important purpose served by FISA's intelligence function. *See, e.g., Kashmiri*, 2010 U.S. Dist. LEXIS 119470, at *9 ("No requirement exists to show probable cause of presently occurring or past criminal activity").

The Supreme Court has stated that "[d]ifferent standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens." *Keith,* 407 U.S. at 322-23 (recognizing that domestic security surveillance "may involve different policy and practical considerations than the surveillance of 'ordinary crime'"). In *Keith,* the Supreme Court acknowledged that: (1) the "focus of . . . surveillance [in domestic security investigations] may be

less precise than that directed against more conventional types of crime"; (2) unlike ordinary criminal investigations, "the gathering of security intelligence is often long range and involves the interrelation of various sources and types of information;" and (3) the "exact targets of such surveillance may be more difficult to identify" than in surveillance operations of ordinary crimes under Title III. *Id.* Although *Keith* was decided before FISA's enactment and addressed purely domestic security surveillance, the rationale underlying *Keith* applies *a fortiori* to foreign intelligence surveillance, where the Government's interest, at least from a national security perspective, would typically be more pronounced.

FISA was enacted partly in response to *Keith.* In constructing FISA's framework, Congress addressed *Keith's* question whether departures from traditional Fourth Amendment procedures "are reasonable, both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens," and "concluded that such departures are reasonable." *See* S. Rep. No. 95-701, 95th Cong., 2d Sess., at 11, (quoting *Keith* at 323) *reprinted in* 1978 U.S.C.C.A.N. 3973, 3980 (1978) ("Senate Report"). Similarly, many courts – including the Foreign Intelligence Surveillance Court of Review – have relied on *Keith* in holding that FISA collection conducted pursuant to a FISC order is reasonable under the Fourth Amendment. *See In re Sealed Case,* 310 F.3d 717, 738, 746 (FISC of Rev. 2002) (finding that while many of FISA's requirements differ from those in Title III, few of those differences have constitutional relevance); *Duggan,* 743 F.2d at 73-74 (holding that FISA does not violate the Fourth Amendment); *see also Ning Wen,* 477 F.3d at 898 (holding that FISA is constitutional despite using "a definition of 'probable cause' that does not depend on whether a domestic crime has been committed"); *Damrah,* 412 F.3d at 624 (denying as meritless the defendant's claim that FISA's

procedures violate the Fourth Amendment); *Pelton,* 835 F.2d at 1075 (finding FISA's procedures compatible with the Fourth Amendment); *Cavanagh,* 807 F.2d at 790-91 (holding that FISA satisfies the Fourth Amendment requirements of probable cause and particularity); *Isa*, 923 F.2d at 1302 (affirming district court's conclusion that FISA collection did not violate the Fourth Amendment and rejecting defendant's challenge to FISA's lower probable cause threshold); *Warsame*, 547 F. Supp. 2d at 993-94 (holding that FISA's probable cause and particularity requirements satisfy the reasonableness requirement of the Fourth Amendment); *Mubayyid,* 521 F. Supp. 2d at 135-41 (rejecting claim that FISA violates the Fourth Amendment's judicial review, probable cause, notice, and particularity requirements); *Falvey,* 540 F. Supp. at 1311-14 (finding that FISA procedures satisfy the Fourth Amendment's warrant requirement).

b. Alternatively, FISA Collection is Subject to the "Good-Faith" Exception

Even assuming *arguendo* that this Court determines that a particular FISC order was not supported by probable cause, or that one or more of the FISA certification requirements were not in fact met, the Government respectfully submits that the FISA materials – and the evidence obtained or derived from the FISA collection – are, nonetheless, admissible under the "good faith" exception to the exclusionary rule articulated in *United States v. Leon,* 468 U.S. 897 (1984). The Seventh Circuit, relying on *Leon,* held that federal officers were entitled to rely in good faith on a FISA warrant. *Ning Wen,* 477 F.3d at 897. As the court noted:

> [T]he exclusionary rule must not be applied to evidence seized on the authority of a warrant, even if the warrant turns out to be defective, unless the affidavit supporting the warrant was false or misleading, or probable cause was so transparently missing that "no reasonably well trained officer [would] rely on the warrant."

Id. (quoting *Leon)* (alteration in original); *see also Duggan,* 743 F.2d at 77 n.6 (opining that *Franks* principles apply to review of FISA orders); *Ahmed,* 2009 U.S. Dist. LEXIS 120007, at *25 n.8 ("[t]he FISA evidence obtained. . . .would be admissible under *Leon's* 'good faith' exception to the exclusionary rule were it not otherwise admissible under a valid warrant").[16]

IV. THE FISA COLLECTION WAS LAWFULLY AUTHORIZED AND CONDUCTED

A. THE FISA COLLECTION WAS LAWFULLY AUTHORIZED

1. The Certifications

Each FISA application was supported by a certification signed by a duly-authorized, high-ranking official of the United States Government. The FISC properly determined that each of those certifications complied with FISA's requirements: *i.e.,* that: (1) the certifying official deemed the information sought to be foreign intelligence information; (2) a significant purpose of the surveillance or search was to obtain foreign intelligence information; and (3) the information sought could not reasonably have been obtained by normal investigative techniques. *See* 50 U.S.C. §§ 1804(a)(6)(A)-(C), 1823(a)(6)(A)-(C). As noted above, certifications submitted in support of a FISA application should be "presumed valid," and neither the FISC nor a reviewing district court should "second-guess the executive branch official's certification that the objective of the surveillance is foreign intelligence information." *Duggan,* 743 F.2d at 77 n. 6; *Gowadia,* 2009 U.S. Dist. LEXIS 47833, at *12. In reviewing the certifications, a district court should apply

[16] The good-faith exception to the exclusionary rule precludes the suppression of evidence obtained or derived from FISA electronic surveillance and/or physical search even if FISA "were deemed unconstitutional" where "there appears to be no issue as to whether the government proceeded in good faith and in reasonable reliance on the FISA orders [because] [t]he exclusionary rule would . . . not . . . apply under the [*Leon*] rule." The good-faith exception "applies when an officer conducts a search in objectively reasonable reliance on the constitutionality of a statute that subsequently is declared unconstitutional." *Arizona v. Evans,* 514 U.S. 1, 13 (1995).

the same standard as the FISC, which is the "clearly erroneous" standard. *Badia,* 827 F.2d at 1463. As discussed below, there is ample information both in the certifications themselves and in the declarations, to demonstrate that the certifications were not clearly erroneous.

a. Foreign Intelligence Information

b. "A Significant Purpose"

c. Information Not Reasonably Obtainable Through Normal Investigative Techniques

For the above reasons, the FISC properly found that the certifications were not clearly erroneous.

B. THE INSTANT FISA COLLECTION MET FISA'S PROBABLE CAUSE STANDARD

D. THE FISA COLLECTION WAS LAWFULLY CONDUCTED

This Court's *in camera* and *ex parte* review of the FISA materials will demonstrate not only that the FISA collection was lawfully authorized, but also that it was lawfully conducted. That is, the FISA-obtained and -derived information that will be offered into evidence in this case was acquired and retained by the FBI in accordance with FISA's minimization requirements, and the implementing SMP's promulgated by the Attorney General and approved by the FISC.

1. Minimization

Under FISA and both sets of SMPs, minimization "may occur at any of several stages, including recording, logging, indexing, or dissemination." *Kevork,* 634 F. Supp. at 1017; *IARA,* 2009 U.S. Dist. LEXIS 118505, at *17; Senate Report at 40; current SMPs, Section I.A., pp. 1-2. At the acquisition stage, FISA does not "prohibit the use of automatic tape recording equipment." *Rahman,* 861 F. Supp. at 252; *Kevork, Id.* Indeed, the FISC has noted that FISA surveillance

devices are normally left on continuously and that consequently minimization occurs (under the old SMPs) during the logging and indexing of the pertinent communications.[17] *See In re Sealed Case*, 310 F.3d at 740.

Generally, after a communication is collected and reduced to an intelligible form (*e.g.*, by transcription or translation), it is reviewed to determine whether it contains, or might contain, foreign intelligence information. *See In re All Matters Submitted to FISC,* 218 F. Supp. 2d 611, 618 (Foreign Intel. Surv. Ct. 2002); *rev'd on other grounds by In re Sealed Case,* 310 F.3d at 717. If it does contain such foreign intelligence information, or is necessary to understand or asses foreign intelligence information, the communication is not subject to minimization; *i.e.,* it meets the standard for retention. Moreover, FISA expressly states that the Government is not required to minimize information that is "evidence of a crime," whether or not it is also foreign intelligence information. 50 U.S.C. § 1801(h)(3); *see also Isa,* 923 F.2d at 1305.

The degree to which information is required to be minimized varies somewhat given the specifics of a particular investigation, such that less minimization at acquisition and retention is justified when "the investigation is focusing on what is thought to be a widespread conspiracy" and more extensive surveillance is necessary "to determine the precise scope of the enterprise." *In re Sealed Case,* 310 F.3d at 741; *United States v. Bin Laden,* 126 F. Supp. 2d at 286 ("[m]ore extensive monitoring and 'greater leeway' in minimization efforts are permitted in a case [involving] . . . [a] 'world-wide, covert and diffuse . . . international terrorist group.'"). Furthermore, the activities of foreign powers and their agents are often not obvious from an initial

[17] "Pertinent communications" refers to those communications that could contain foreign intelligence information or evidence of a crime.

or cursory overhear of conversations. To the contrary, agents of foreign powers frequently engage in coded communications, compartmentalized operations, the use of false identities and other practices designed to conceal the breadth and aim of their operations, their organization, activities and plans. *See, e.g., United States v. Salameh,*152 F.3d 88, 154 (2d Cir. 1998) (noting that two conspirators involved in the 1993 bombing of the World Trade Center in New York referred to the bomb plot as the "study" and to terrorist materials as "university papers"). As one court explained, "[i]nnocuous-sounding conversations may in fact be signals of important activity [and] information on its face innocent when analyzed or considered with other information may become critical." *Kevork,* 634 F. Supp. at 1017 (quoting House Report at 55); *see also In re Sealed Case,* 310 F.3d at 740-41; *Bin Laden,* 126 F. Supp. 2d at 286. Likewise, "individual items of information, not apparently significant when taken in isolation, may become highly significant when considered together over time." *Kevork,* 634 F. Supp. at 1017; *Rahman,* 861 F. Supp. at 252-53 (rejecting the notion that the "wheat" could be separated from the "chaff" while the "stalks were still growing"). This is especially true where the individuals involved use codes or cryptic language. See e.g., *Hammoud,* 381 F.3d at 334 ("[a] conversation that seems innocuous on one day may later turn out to be of great significance, particularly if the individuals involved are talking in code"); *Bin Laden,* 126 F. Supp. 25 at 286; *Kevork,* 634 F. Supp. at 1017; *Thomson,* 752 F.Supp. at 81 (permissible to retain and disseminate "bits and pieces" of information until their "full significance becomes apparent"). As a result, "courts have construed 'foreign intelligence information' broadly and sensibly allowed the government latitude in its determination of what is foreign intelligence information." *Rosen,* 447 F. Supp. 2d at 551; *IARA,* 2009 U.S. Dist. LEXIS 118505, at *18.

Moreover, as noted above, FISA expressly states that the Government is not required to minimize information that is "evidence of a crime." 50 U.S.C. §§ 1801(h)(3), 1821(4)(c). As a result, to the extent that certain communications of a United States person may be evidence of a crime or may otherwise establish an element of a substantive or conspiratorial offense, such communication need not be minimized. *Isa*, 923 F.2d at 1305.

The nature of the foreign intelligence information sought also impacts the amount of information regarding a United States person that can properly be retained and disseminated. As Congress explained, there is a legitimate need to conduct a thorough post-acquisition review of FISA information that involves a United States person who is acting as an agent of a foreign power:

> It is "necessary" to identify anyone working with him in this network, feeding him information, or to whom he reports. Therefore, it is necessary to acquire, retain and disseminate information concerning all his contacts and acquaintances and his movements. Among his contacts and acquaintances, however, there are likely to be a large number of innocent persons. Yet, information concerning these person must be retained at least until it is determined that they are not involved in the clandestine intelligence activities and may have to be disseminated in order to determine their innocence.

House Report at 58. Indeed, courts have cautioned that, when a United States person communicates with an agent of a foreign power, the Government would be "remiss in meeting its foreign counterintelligence responsibilities" if it did not thoroughly "investigate such contacts and gather information to determine the nature of those activities." *Thomson,* 752 F.Supp. at 82.

Congress also recognized that agents of a foreign power are often very sophisticated and skilled at hiding their activities. *See Thomson,* 752 F. Supp. at 81 (quoting House Report at 58). Accordingly, to pursue leads, Congress intended that the Government be given "a significant

degree of latitude" with respect to the "retention of information and the dissemination of information between and among counterintelligence components of the Government." *Id.*

In light of these realities, Congress recognized that minimization efforts by the Government can never be free of mistake, because "no electronic surveillance can be so conducted that innocent conversations can be totally eliminated." Senate Report at 39. The Fourth Circuit reached the same conclusion in *Hammoud,* 381 F.3d at 334, stating that the "mere fact that innocent conversations were recorded, without more, does not establish that the government failed to appropriately minimize surveillance".[18] Accordingly, in reviewing the adequacy of minimization efforts, the test to be applied is neither whether innocent conversations were intercepted, nor whether mistakes were made with respect to particular communications. Rather, as the United States Supreme Court stated in the context of Title III surveillance, there should be an "objective assessment of the [agents'] actions in light of the facts and circumstances confronting [them] at the time." *Scott v. United States,* 436 U.S. 128, 136 (1978). The test of compliance is whether a good faith effort to minimize was made. *Hammoud,* 381 F.3d at 334 ("[t]he minimization requirement obligates the Government to make a good faith effort to minimize the acquisition and retention of irrelevant information"); *see also* Senate Report at 39-40 (stating that the court's role is to determine whether "on the whole, the agents have shown a high regard for the right of privacy and have done all they reasonably could do to avoid unnecessary intrusion"); *IARA,* 2009 U.S. Dist. LEXIS 118505, *18-19 (quoting Senate Report at 39-40).

[18] The reason is that although "the minimization requirement obligates the Government to make a good faith effort to minimize . . . it is not always immediately clear into which category a particular conversation falls. A conversation that seems innocuous on one day may later turn out to be of great significance, particularly, if the individuals involved are talking in code." *Hammoud,* 381 F.3d at 334, citing Senate Report at 39-40.

Moreover, absent evidence that there has been a complete disregard for the minimization procedures, suppression is not the appropriate remedy with respect to those communications that were properly obtained and retained. Indeed, Congress intended that any suppression remedy should apply only to the "evidence which was obtained unlawfully." House Report at 93. FISA's legislative history reflects that Congress intended only this limited sanction for errors of minimization:

> As the language of the bill makes clear, only that evidence which was obtained unlawfully or derived from information obtained unlawfully would be suppressed. If, for example, some information should have been minimized but was not, only that information should be suppressed; the other information obtained lawfully should not be suppressed.

Id; *accord IARA*, 2009 U.S. Dist. LEXIS 118505, at *20-21 ("this Court declines to suppress evidence obtained through FISA warrants properly issued and conducted"); *see also United States v. Falcone*, 364 F.Supp. 877, 886-87 (D.N.J. 1973), *aff'd* 500 F.2d 1401 (3rd Cir. 1974) (Title III).

2. The FISA Collection was Appropriately Minimized

V. CONCLUSION

Defendants' motions should be denied. Courts have uniformly held that the probable cause requirement of FISA comports with the requirements of the Fourth Amendment to the United States Constitution, *see, e.g., Isa*, 923 F.2d at1304; and that FISA's provisions for *in camera, ex parte* review comport with the due process requirements of the United States Constitution. See, *e.g. Spanjol,* 720 F.Supp. at 58-59; *United States v. Butenko,* 494 F.2d 593, 607 (3d Cir.), *cert denied sub nom, Ivanov v. United States*, 419 U.S. 881 (1974); *Damrah*, 412 F.3d at 624; *Warsame*, 547 F. Supp. 2d at 988-89. The defendants advance no argument to justify any deviation from this well-established precedent.

Even if this Court were to determine that the FISA collection had not been lawfully authorized or lawfully conducted, the FISA evidence would nevertheless be admissible under the "good faith" exception to the exclusionary rule articulated in *Leon*, 468 U.S. 897 (1984). *See also Ning Wen*, 477 F.3d at 897 (holding that the *Leon* good-faith exception applies to FISA orders); *Mubayyid*, 521 F.Supp.2d at 140 n. 12 (noting that the Government could proceed in good-faith reliance on FISA orders even if FISA were deemed unconstitutional); *Ahmed*, 2009 U.S. Dist. Lexis 120007, at *25 n. 8; *Nicholson*, U.S. Dist. LEXIS 45126 at *17.

The Attorney General has filed a declaration in this case stating that disclosure or an adversary hearing would harm the national security of the United States. Therefore, FISA mandates that this Court conduct an *in camera* and *ex parte* review of the challenged FISA materials to determine whether the collection was both lawfully authorized and conducted. In conducting that review, the Court may disclose the FISA materials "only where such disclosure is necessary to make an accurate determination of the legality of the surveillance [or search]." *See* 50 U.S.C. §§ 1806(f), 1825(g). Congress, in enacting FISA's procedures for *in camera, ex parte* judicial review, has balanced and accommodated the competing interests of the Government and criminal defendants, and has articulated the proper standard for disclosure; that is, only where the Court finds that disclosure is necessary to the Court's accurate determination of the legality of the FISA collection. *See id.* The Court will be able to render a determination based on its *in camera, ex parte* review, and the defendant has failed to present any colorable basis for supplanting Congress' reasoned judgment with a different proposed standard of review.

The Government respectfully submits that the Court can make this determination without disclosing the classified and highly-sensitive FISA materials to the defendant. Every federal court

that has been asked to determine the legality of a FISC-authorized collection has been able to do so *in camera* and *ex parte* and without the assistance of defense counsel. The FISA materials at issue here are organized and readily understood, and an overview of them is presented hereinafter as a frame of reference.

Based on the foregoing analysis and a review of the materials submitted *in camera* and *ex parte,* the Government respectfully submits that the Court should: (1) conduct an *in camera* and *ex parte* review of the FISA dockets and the Government's classified submission; (2) find that the FISA surveillance was lawfully authorized and lawfully conducted in compliance with the Fourth Amendment; (3) hold that disclosure of the FISA dockets and the Government's classified submissions to the defense is not required because the Court is able to make an accurate determination of the legality of the surveillance without disclosing the FISA dockets or any portions thereof; (4) order that the FISA dockets and the Government's classified submissions be maintained under seal by the Court Security Officer or his/her designee; and (5) deny the defendants' Motions. [19]

[19] A district court order requiring the disclosure of FISA materials is a final order for purposes of appeal. See 50 U.S.C. § 1806(h). In the unlikely event that the Court concludes that disclosure of any item within any of the FISA materials may be required, given the significant national security consequences that would result from such disclosure, the Government would expect to pursue an appeal. Accordingly, the Government respectfully requests that the Court indicate its intent to do so before issuing any order, or that any such order be issued in such a manner that the United States has sufficient notice to file an appeal prior to any actual disclosure.

Respectfully submitted,

GEORGE B. HOLDING
United States Attorney

By: /s/ John S. Bowler

JOHN BOWLER
BARBARA KOCHER
Assistants United States Attorney
310 New Bern Avenue, Suite 800
Raleigh, NC 27601
Tel: (919) 856-4301
Fax: (919) 856-4487
Email: john.bowler@usdoj.gov
NC Bar No. 18825
Email: barb.kocher@usdoj.gov
NC Bar No. 16360

/s/ Jason M. Kellhofer

JASON M. KELLHOFER
Trial Attorney
Counterterrorism Section
National Security Division
U.S. Department of Justice
10th St. & Pennsylvania Ave., N.W.
Washington D.C. 20530
Tel: (202) 353-7371
Fax: (202) 353-0778
Email: jason.kellhofer@usdoj.gov
OH Bar No. 0074736

Dated: May 23, 2011

CERTIFICATE OF SERVICE

This is to certify that I have this 31st day of May, 2011, served a copy of the foregoing upon counsel for the defendants in this action by electronically filing the foregoing with the Clerk of Court, using the CM/ECF:

Rosemary Godwin
and Debra C. Graves
Federal Public Defender
150 Fayetteville St. Mall
Suite 450
Raleigh , NC 27601-2919

Robert J. McAfee
McAfee Law, P.A.
P. O. Box 905
New Bern , NC 28563

Paul Sun
P.O. Box 33550
Raleigh, NC 27636

Myron T. Hill , Jr.
Browning & Hill
200 E. Fourth St.
Greenville , NC 27835

R. Daniel Boyce
Nexsen Pruet, PLLC
4141 Parklake Ave., Suite 200
P. O. Box 30188
Raleigh, NC 27612

James M. Ayers, II
307 Metcalf Street
Post Office Box 1544
New Bern, North Carolina 28563

Joseph E. Zeszotarski, Jr.
Poyner & Spruill
PO Box 1801
Raleigh, NC 27602

and further, upon defendant Anes Subasic by placing a copy postage pre-paid in first class mail addressed to: Anes Subasic, Public Safety Center, Attn: Wake County Jail, Post Office 2419, Raleigh, NC 27602.

/s/ John S. Bowler
BY: JOHN S. BOWLER
Assistant United States Attorney
Criminal Division
310 New Bern Avenue, Suite 800
Raleigh, NC 27601
Telephone: 919-856-4530
Fax: 919-856-4487
E-mail: john.s.bowler@usdoj.gov